Uma imagem com texto

Descrição gerada automaticamente

TeSP de CiberSegurança e Redes Informáticas

Lourenço Eduardo Estêvão Pereira Índio – 2231606

Diogo Miguel Lucas Garcia - 2231620

Antonio

Trabalho da Unidade Curricular de SRS

Leiria, novembro de 2024

# Lista de Imagens

**Não foi encontrada nenhuma entrada do índice de ilustrações.**

# Lista de siglas e acrónimos

|  |  |
| --- | --- |
| ESTG | Escola Superior de Tecnologia e Gestão |
| IPLeiria | Instituto Politécnico de Leiria |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Índice

[Lista de Imagens ii](#_Toc181801047)

[Lista de siglas e acrónimos iii](#_Toc181801048)

[1. Introdução 1](#_Toc181801049)

[1.1. Objetivo do trabalho 1](#_Toc181801050)

[2. Caso de Estudo 2](#_Toc181801051)

[2.1. Serviço de Email 2](#_Toc181801052)

[2.2. Serviço de Monitorização 2](#_Toc181801053)

[2.3. Serviço de Acesso Remoto 2](#_Toc181801054)

[3. Serviços de Rede Seguros 4](#_Toc181801055)

[3.1. Serviço de nomes (DNS) 4](#_Toc181801056)

[3.1.1. Funcionalidade do DNS em uma Empresa 4](#_Toc181801057)

[3.1.2. BIND (Berkeley Internet Name Domain) 5](#_Toc181801058)

[3.1.3. Como é que isto reforça a segurança? 6](#_Toc181801059)

[3.2. Serviço Web (Apache2) 6](#_Toc181801060)

[3.2.1. Software Apache 6](#_Toc181801061)

[3.2.2. Virtual Hosts 6](#_Toc181801062)

[3.2.3. Segurança 7](#_Toc181801063)

[3.2.4. Criação de contas de serviços e permissões 7](#_Toc181801064)

[3.3. Configuração e gestão de tarefas de registo de eventos, monitorização e auditoria. 7](#_Toc181801065)

[3.3.1. Registo de eventos 8](#_Toc181801066)

[3.3.2. Monitorização e auditoria 8](#_Toc181801067)

[3.3.3. Definição da hora 8](#_Toc181801068)

[4. Conclusões 9](#_Toc181801069)

[5. Bibliografia 10](#_Toc181801070)

# Introdução

Neste relatório, apresenta-se a fase inicial do desenvolvimento de uma rede e serviços para uma empresa Este projeto visa estabelecer um ambiente seguro e eficiente, correspondendo às necessidades de uma empresa que lida com clientes, serviços, rede e servidores.

## Objetivo do trabalho

Este trabalho será realizado no âmbito da UC de SRS do curso CRI e tem por objetivo, desenvolver uma infraestrutura de rede e serviços segura e eficiente para a empresa uma determinada empresa. Deve permitir que a empresa ofereça suas soluções e plataformas com confiabilidade e segurança.

Serão configurados e implementados serviços essenciais que achamos essenciais como: Serviços de rede e conectividade para garantir uma comunicação segure entre utilizadores, serviços de acesso remoto para facilitar a gestão de maneira mais segura.

# Caso de Estudo

## Serviço de Email

O serviço de email é essencial para a comunicação interna e externa de qualquer empresa, permite que os colaboradores enviem e recebam emails de forma segura, seja para comunicação interna ou para contato com clientes externos.

Contas:

## Serviço de Monitorização

O serviço de monitorização é crucial para garantir a operação contínua e eficiente dos sistemas e serviços da empresa, permite que a equipe de TI acompanhe o desempenho, a disponibilidade e a integridade dos recursos de rede, detetando e respondendo rapidamente a possíveis problemas ou falhas que poderão acontecer.

Para implementar este serviço, iremos utilizar o NAGIOS, é um serviço popular e confiável para monitorizar a rede e servidores. O NAGIOS permite monitorizar vários aspetos dos sistemas bem como: disponibilidade de serviços, desempenho de recurso e até mesmo enviar alertas de possíveis problemas.

## Serviço de Acesso Remoto

O serviço de acesso remoto permite que os administradores gerenciem os servidores de forma segura, podendo os mesmos estar fora das instalações da empresa. Esse acesso é fundamental para realizar tarefas de manutenção, atualização e resposta a incidentes de forma rápida e eficiente.

O OpenSSH é um software de acesso remoto, devido à sua segurança e flexibilidade ele é amplamente utilizado para conexões seguras, permitindo o acesso a servidores via protocolo SSH (Secure Shell).

**Configurações de Segurança**:

* **Autenticação por Chave SSH**: A autenticação será feita através da chave SSH, que são mais seguras. Somente usuários com a chave privada irão conseguir ter acesso aos servidores.
* **Criptografia RSA**: Será utilizada a criptografia RSA para a geração das chaves, garantindo assim um nível de alta segurança.
* **Tamanho da Chave**: A chave será gerada com um tamanho de 4096 bits
* **Armazenamento da Chave Privada**: A chave privada será armazenada com segurança pelos administradores da rede, em dispositivos seguros e protegidos por senha, para evitar que seja acedida por terceiros.

**Quem vai utilizar?**

O acesso remoto será distribuído aos administradores do sistema responsáveis pela manutenção e monitorização dos servidores. Cada utilizador autorizado terá sua própria chave SSH, permitindo auditoria e controle de acesso.

# Serviços de Rede Seguros

## Serviço de nomes (DNS)

O serviço de nomes ou DNS (Domain Name System), é responsável pela resolução de nomes de domínio em endereços IP, permitindo que os utilizadores acesse aos serviços e sites da empresa por meio de nomes em vez de endereços IP numéricos. Esse serviço é essencial para a navegação e comunicação em rede, tanto para acesso interno quanto externo.

### Funcionalidade do DNS em uma Empresa

Para uma empresa, o DNS é vital tanto para o **acesso interno quanto externo** aos serviços:

* **Acesso Interno**: Facilita a navegação dentro da rede corporativa, permitindo que funcionários acedam os recursos internos (como servidores de arquivos e intranet) usando nomes amigáveis em vez de endereços IP.

**Acesso Externo**: Permite que clientes e parceiros acedam serviços da empresa hospedados em servidores públicos (por exemplo, site da empresa, e-mail, e-commerce).

### BIND (Berkeley Internet Name Domain)

O BIND (Berkeley Internet Name Domain) é um software de DNS, pois é um dos mais populares e confiáveis para implementação de serviços DNS, com suporte para as principais funcionalidades de segurança e redundância. Algumas das principais funcionalidades que fazem do BIND uma escolha popular incluem:

1. **Suporte a Zonas Primárias e Secundárias**:
   * O BIND permite configurar **servidores DNS primários e secundários**, garantindo **redundância** e **disponibilidade**. Se o servidor DNS primário falhar, o secundário pode continuar respondendo às consultas.
2. **Segurança com DNSSEC**:
   * **DNSSEC** (DNS Security Extensions) é uma extensão de segurança que protege o DNS contra ataques como envenenamento de cache e falsificação de dados, assegurando a **autenticidade e integridade das respostas DNS**.
3. **Controlo de Acesso com ACLs**:
   * O BIND permite definir **ACLs** (Access Control Lists) para controlar quem pode consultar, transferir zonas ou atualizar registros DNS. Isso ajuda a proteger o DNS contra acessos não autorizados e pode ser configurado para permitir apenas consultas de dispositivos internos, se necessário.
4. **Balanceamento de Carga e Alta Disponibilidade**:
   * Com o uso de **registros DNS de balanceamento de carga** (como registros de tipo *A* com múltiplos IPs), o BIND pode distribuir o tráfego entre vários servidores, proporcionando **distribuição de carga** e **melhor desempenho**.
5. **Log e Monitoramento**:
   * O BIND oferece recursos extensivos de **log** e **monitoramento**, permitindo que os administradores acompanhem as consultas DNS, identifiquem problemas, e ajustem a configuração para otimizar o desempenho e a segurança.
6. **Zonas e Registros:**
   * Zona de Forward (.com): Contém registros para os serviços e servidores acessíveis externamente.
   * Zona de Reverse (ex. 192.168.24.5): Permite a resolução reversa para identificar nomes a partir de endereços IP internos.

|  |  |  |
| --- | --- | --- |
| Tipo de Registro | Nome | IP |
| A | .com | 192.168.24.10 |
| MX | mail | 192.168.20.20 |
| NS | ns1 | 192.168.20.30 |

### Como é que isto reforça a segurança?

Globalmente, essas configurações reforçam a segurança do serviço DNS ao proteger a integridade, disponibilidade e controle de acesso.

## Serviço Web (Apache2)

Um serviço web permite que pessoas acessem sites e aplicativos de uma empresa pelo navegador. É o que faz o site aparecer na tela quando alguém acede o endereço da empresa.

### Software Apache

Apache é um programa usado para configurar e gerenciar serviços web, permitindo a hospedagem de sites e aplicativos de maneira confiável e personalizável.

### Virtual Hosts

Com o Apache, é possível configurar múltiplos sites ou serviços na mesma máquina, cada um com suas próprias configurações, como endereços e permissões.

### Segurança

* **HTTPS**: Criptografa a comunicação entre o servidor e o usuário para garantir a segurança dos dados.
* **Autenticação Básica**: Restringe o acesso a certas áreas do site, exigindo que o usuário insira um nome de usuário e senha.
* **Forçar HTTPS**: Redireciona automaticamente todos os acessos para uma conexão segura, protegendo os dados durante o tráfego na rede.

### Criação de contas de serviços e permissões

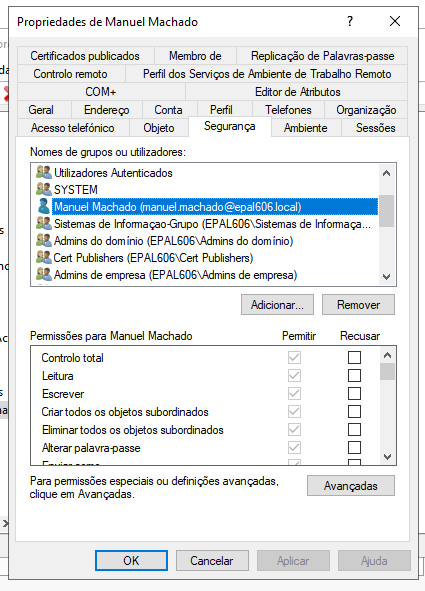


Imagem 15 - Permissões

## Configuração e gestão de tarefas de registo de eventos, monitorização e auditoria.

A configuração e gestão de registos de eventos, monitoramento contínuo e auditorias regulares são importantes para a segurança e integridade dos sistemas de informação. A definição de eventos a serem registados, a deteção de anomalias protege os dados e assegura a continuidade de um bom serviço.

### Registo de eventos

O registo de eventos é uma funcionalidade que captura e armazena informações sobre eventos e atividades que ocorrem em um sistema, como por exemplos erros, alertas, informações de segurança, alterações de configuração entre outras.

### Monitorização e auditoria

A monitorização e a auditoria são práticas essenciais para garantir a segurança, desempenho e conformidade de um ambiente de tecnologia da informação. Elas envolvem o acompanhamento contínuo das atividades, eventos e métricas de sistemas.

### Definição da hora

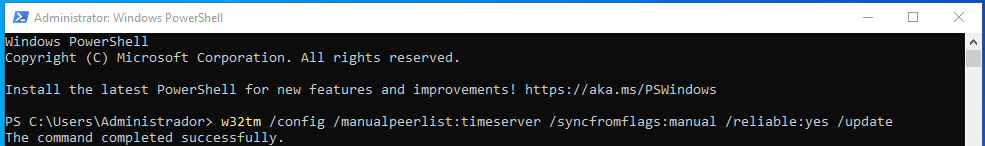


Imagem 16 - Definição da Hora

# Conclusões

Concluir esta etapa foi importante para compreender os conceitos básicos do Windows Server, algumas configurações a implementar. Na minha opinião é importante saber primeiros estes conceitos para depois passar para a prática, e assim fica muito mais fácil saber o que estamos a fazer. Existem algumas funcionalidades e regras que não foram implementadas como por exemplo separar os Users dos Computadores que serão implementadas na segunda etapa. A maior dificuldade sentida foi na delegação de tarefas.

# Bibliografia

<https://www.alitajran.com/create-active-directory-users-from-csv-with-powershell/>

<https://www.linkedin.com/pulse/explorando-os-fundamentos-e-aplica%C3%A7%C3%B5es-da-anderson-vieira-machado-1nxuf/?originalSubdomain=pt>

<https://www.linkedin.com/pulse/boas-pr%C3%A1ticas-de-seguran%C3%A7a-para-m%C3%A1quinas-virtuais-em-nuvem-ag%C3%A1pto/?originalSubdomain=pt>

<https://pt.wikipedia.org/wiki/VirtualBox>

<https://www.vmware.com/pdf/ws_specs_pt.pdf>